REMARKS/ARGUMENTS

1.) Allowable Subject Matter

The Examiner objected to claim 14, but indicated it would be allowable if rewritten in independent form, including all of the limitations of the base claim and any intervening claims. The Applicant thanks the Examiner for the indication of allowable subject matter. The Applicant, however, believes that claim 11, from which claim 14 is dependent, is allowable over the cited prior art. The Applicant, therefore, declines to so amend claim 14.

2.) Claim Rejections – 35 U.S.C. §103(a)

The Examiner rejected claims 11, 25, 16, 18 and 20 as being unpatentable over Reich, *et al.* (US 2002/0184256 A1) in view of Matsumoto, *et al.* (US 6,711,264); claims 12 and 13 as being unpatentable over Reich in view of Matsumoto and further in view of Pant, *et al.* (US 6,931,543); and claims 17 and 19 as being unpatentable over Reich in view of Matsumoto and further in view of D'Amico, *et al.* (US 5,077,790). The Applicant traverses the rejections.

Claim 11 recites:

> 11. A method of controlling a network entity of a mobile communication network and a mobile station, wherein said network entity and said mobile station are adapted to conduct a plurality of predetermined message exchange procedures in the course of which predetermined messages are exchanged between said network entity and said mobile station depending on the given procedure, where said predetermined messages may be encrypted, an encrypted message being any message of which at least a part is encrypted, and where said network entity and said mobile station are adapted to conduct one or more encryption key generation procedures during which the network entity and the mobile station generate and store respective corresponding encryption keys in order to be able to encrypt and decrypt exchanged messages, said method comprises the steps of:
>
> if said network entity receives a message from said mobile station, determining whether said received message is encrypted;
>
> <u>if the received message is encrypted</u>, determining whether a correct encryption key for decrypting said message is available to said network entity <u>and, if no correct key is available, sending a predetermined triggering message to said mobile station</u>; <u>and</u>

> upon receiving said predetermined triggering message, said mobile station interrupting the procedure in the course of which it sent the encrypted message for which the network entity did not have a correct key, and initiating an encryption key generation procedure. (emphasis added).

Wish respect to claim 11, the Examiner recognizes the deficiencies in the teachings of Reich. Specifically, the Examiner recognizes that Reich fails to teach that "if [a] received message [from a mobile station] is encrypted, determining whether a correct encryption key for decrypting [the] message is available . . . and, if no correct key is available, sending a predetermined triggering message to [the] mobile station," and "upon receiving [the] predetermined triggering message, [the] mobile station interrupting the procedure in the course of which it sent the encrypted message for which the network entity did not have a correct key, and initiating an encryption key generation procedure." To overcome those deficiencies, the Examiner looks to the teachings of Matsumoto.

Matsumoto, however, also fails to teach the novel limitations recited in claim 11. The Examiner asserts that Matsumoto "inherently" teaches those limitations, pointing to the procedure described at column 2, lines 11-24. That portion of Matsumoto, however, only describes the conventional prior art procedure for the exchange of encryption keys between devices **prior to** the exchange of encrypted messages between such devices. In contrast, Applicant's invention solves a problem in such prior art solutions when it is determined **after** an encrypted message has already been sent/received that the receiving device does not have the necessary key to decrypt the message. As described by Applicant at page 8, line 23, to page 9, line 28, of the application, the claimed invention eliminates the delays that result in such a situation using the procedures of the prior art. Matsumoto fails to address this problem, much less suggest that it would be desirable to send a "triggering message," as claimed by Applicant, to cause the interruption of a procedure in which an encrypted message was sent by a mobile station and, thereby, initiate an encryption key generation procedure. Therefore, Matsumoto fails to cure the deficiencies of Reich and, thus, the Examiner has not established a *prima facie* case of obviousness of claim 11.

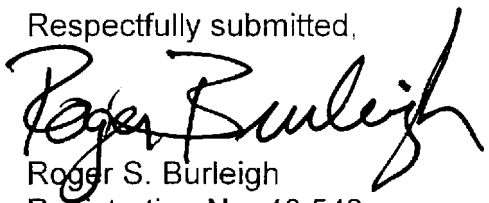
Whereas claims 18 and 20 recite analogous limitations to the novel aspects of claim 11, the Examiner has also not established a *prima facie* case of obviousness of those claims. Furthermore, whereas claims 12-17 and 19 are dependent from claims 11 and 18, respectively, and include the limitations thereof, those claims are also not obvious.

CONCLUSION

In view of the foregoing remarks, the Applicant believes all of the claims currently pending in the Application to be in a condition for allowance. The Applicant, therefore, respectfully requests that the Examiner withdraw all rejections and issue a Notice of Allowance for claims 11-20.

The Applicant requests a telephonic interview if the Examiner has any questions or requires any additional information that would further or expedite the prosecution of the Application.

Respectfully submitted,



Roger S. Burleigh
Registration No. 40,542

Date: June 29, 2006

Ericsson Inc.
6300 Legacy Drive, M/S EVR 1-C-11
Plano, Texas 75024

(972) 583-5799
roger.burleigh@ericsson.com